EXHIBIT A

Fulton County Superior Court
EFILEDDC
Date: 2/20/2018 1:08 PM
Cathelene Robinson, Clerk

Date of service:
2/27/2018

IN THE SUPERIOR COURT OF FULTON COUNTY, GEORGIA
136 PRYOR STREET, ROOM C-103, ATLANTA, GEORGIA 30303
SUMMONS

WILLIAM H MUSCARELLA
PATRICIA R. MUSCARELLA
Plaintiff,

vs.

EQUIFAX INC.
EQUIFAX INFORMATION SERVICES L.L.C
Defendant

Case No.: 2018CV301393

TO THE ABOVE NAMED DEFENDANT(S):

You are hereby summoned and required to file electronically with the Clerk of said Court at https://efilega.tylerhost.net/ofsweb and serve upon plaintiff's attorney, whose name and address is:

WILLIAM H MUSCARELLA
278 SPRING DRIVE
ROSWELL, GA 30075

An answer to the complaint which is herewith served upon you, within 30 days after service of this summons upon you, exclusive of the day of service; unless proof of service of this complaint is not filed within five (5) business days of such service. Then time to answer shall not commence until such proof of service has been filed. **IF YOU FAIL TO DO SO, JUDGMENT BY DEFAULT WILL BE TAKEN AGAINST YOU FOR THE RELIEF DEMANDED IN THE COMPLAINT.**

This 20TH day of FEB, 2018

Honorable Cathelene "Tina" Robinson
Clerk of Superior Court
By: Lisa M. Reyes
Deputy Clerk

To defendant upon whom this petition is served:
This copy of complaint and summons was served upon you _____, 20_____

_____
Deputy Sheriff

Instructions: Attach addendum sheet for additional parties if needed, make notation on this sheet if addendum is used

Date of service:
2/28/2018

IN THE SUPERIOR COURT OF FULTON COUNTY, GEORGIA
136 PRYOR STREET, ROOM C-103, ATLANTA, GEORGIA 30303
SUMMONS

WILLIAM H MUSCARELLA
PATRICIA R. MUSCARELLA
Plaintiff,

vs.

EQUIFAX INC,
EQUIFAX INFORMATION SERVICES L.L.C
Defendant

) Case No.: 2018CV301393

TO THE ABOVE NAMED DEFENDANT(S):

You are hereby summoned and required to file electronically with the Clerk of said Court at https://efilega.tylerhost.net/ofsweb and serve upon plaintiff's attorney, whose name and address is:

WILLIAM H. MUSCARELLA
278 SPRING DRIVE
ROSWELL, GA 30075

An answer to the complaint which is herewith served upon you, within 30 days after service of this summons upon you, exclusive of the day of service; unless proof of service of this complaint is not filed within five (5) business days of such service. Then time to answer shall not commence until such proof of service has been filed. **IF YOU FAIL TO DO SO, JUDGMENT BY DEFAULT WILL BE TAKEN AGAINST YOU FOR THE RELIEF DEMANDED IN THE COMPLAINT.**

This 20TH day of FEB, 2018

Honorable Cathelene "Tina" Robinson
Clerk of Superior Court
By Lisa M Reyes
Deputy Clerk

To defendant upon whom this petition is served:
This copy of complaint and summons was served upon you _____, 20_____

_____
Deputy Sheriff

Instructions: Attach addendum sheet for additional parties if needed, make notation on this sheet if addendum is used

IN THE SUPERIOUR COURT OF FULTON COUNTY

STATE OF GEORGIA

WILLIAM H. AND PATRICIA R.	)	COMPLAINT
MUSCARELLA, on behalf of themselves,	)	No. _____
Plaintiffs Pro Se	)	JURY TRIAL DEMAND
	)	
V.	)	
EQUIFAX INC., and	)	
EQUIFAX INFORMATION SERVICES	)	
LLC.	)	
Defendants	)	

COMPLAINT FOR DAMAGES

Plaintiff William H. Muscarella and Plaintiff Patricia R. Muscarella ("hereafter Plaintiffs") on behalf of themselves allege the following against Equifax Inc. and Equifax Information Services LLC. ("Hereafter) Defendants and/or Equifax and/or the Company and/or "[its]"), based on personal knowledge and Plaintiffs' information from news reports, Federal and Georgia State statutory laws and/or rules and belief as to the action/s of Equifax and others associated with Equifax and/or the Company and/or [its] Board of Directors.

I. INTRODUCTION

1. Defendants Equifax Inc. and Equifax Information Services LLC operate "Equifax Inc.," a consumer credit reporting agencies located in Atlanta, Georgia of United States America. The Plaintiffs bring this action alleging violations of the Federal Fair Credit Reporting Act, the Georgia Fair Business Practices Act, the Georgia Security Breach Notification Act, as well as statutory/common Law claims for failure, failure per se, breach of Fiduciary Duty of Loyalty, Fiduciary Duty of Care, Fiduciary Duty of Obedience, Fiduciary Duty of Good Faith and Fair Dealing, Fiduciary Duty of Disclosure, Identity Theft, in Violation

of the Fourth Amendment of the United States of America and the demonstrations of "contributory" act/s of negligence with a "willful and wanton" misconduct of negligence by not heeding U. S. Homeland Security Department warning on or about March 8, 2017. The Company's and/or affiliates and/or others unjust enrichment at the Plaintiff's expense and failure to fulfill bailment obligations. Plaintiffs seek declaratory and injunctive relief and redress.

Equifax stole and/or pilfered Plaintiff's sensitive "Personal Identifying Information" (hereinafter the PII), Equifax owed the Plaintiffs various Fiduciary duties which includes the "Duty of Care" to take adequate measures to protect, shield, shelter, safeguard and preserve the PII information which Equifax surreptitiously collected and amassed and produced and stored and management of the Plaintiff's PII without their "verbal" or "written" permission which included the following(but not limited only to the following); private, secret, privileged financial and personal information (social security numbers), material, data and life's history of each Plaintiff.

2. Equifax acknowledges that, between March 2017 and July 2017, Equifax was the subject of a "Data Breach" in which unauthorized individuals accessed Equifax's data base/s and/or computer system/s which contained the Plaintiff's names, "Social Security Numbers", addresses and other PII information of which Equifax pilfered/collected/amassed/produced/managed/ "stored" and "controlled" within Equifax company and/or affiliates on [its] computer system/s and/or data base/s therein (hereinafter the "Data Breach"). According to Equifax, the "Data Breach" affected as many as 143 million people and Equifax "admits" to the unauthorized access; of the latest "Data Breach" occurring in 2017. But, failed to alert Plaintiffs to the fact of such breach. But, on/or about July 29, 2017; Equifax made a Public statement regarding the "Data Breach".

3. The "Data Breach" was the inevitable result of Equifax's inadequate, inept, failed attitude at data security and the protection of the Plaintiff's PII that was surreptitiously collected, amassed, managed, produced and stored regarding the Plaintiff's PII during the course of [its] business. Defendants knew and should have known of the derisory state of [its] own data security system/s. Equifax has experienced similar breaches of PII on smaller scales in the past, including on/or about 2013, 2016 and as recently as on/or about January thru July of 2017. Equifax started business as a credit reporting company in 1913 and grown to be a $1.54 billion dollar origination in 2016. Equifax has jeopardized the PII of the Plaintiffs and thousands of Americans and others for years; as stated by Equifax in [its] public statement on or about July 29, 2017.

4. Despite this long history of breaches, Defendants have failed to prevent a "Data Breach" that has exposed the PII of the Plaintiffs. The damage done to the Plaintiffs may follow them for the rest of their lives, as they will have to monitor closely their financial accounts to detect any fraudulent activity and incur expenses for years to protect, shield and preserve themselves from, and combat, "Identity Theft" now and in the foreseeable future.

5. Equifax knew and should have known the risks associated with having a derisory security system/s of [its] computer system/s and/or data base/s. The potential for harm caused by insufficient safeguards and shields for the Plaintiffs' PII is profound. With data such as that disclosed in the "Data Breach", identity thieves can cause irreparable and long-lasting damage to Plaintiffs, from filing of loans and opening fraudulent bank accounts to selling valuable PII to the highest bidder.

6. In the case of Defendants' "Data Breach", the potential repercussions for Plaintiffs are particularly egregious. Privacy researchers and fraud analysts have called this attack "as bad as it gets." "On a scale of 1 to 10 in terms of risk to Plaintiffs, this is a 10."

7. Equifax was, or should have known, should have been aware of the specific vulnerability in [its] derisory security system/s as early as March 2017. When the Homeland Security Department warned Equifax on/or about March 8, 2017 of an "on line gap" (Apache struts CVE-2017-5638) in [its] U. S. website. Mr. Richard F. Smith (former Chief Executive Officer) stated "but the Company did nothing" while testifying before the House Energy Committee of the United States of America's Congress on or about October 3, 2017. Despite knowing that their system/s' flaw/s was jeopardizing the Plaintiffs PII, Equifax failed to implement an effective patch for about 9 weeks, and failed to check this known vulnerability regularly to ensure Plaintiffs information was secure throughout the period of the "Data Breach".

8. Defendants failed to inform the Plaintiffs of the "Data Breach", but the Defendant's employees did not hesitate to protect themselves; at least three Equifax senior executives, including (Chief Financial Officer) John W. Gamble Jr., upon information and belief, sold Equifax stock shares worth $1.8 million dollars; as well as (President of Work Force Solutions) Joseph Loughran and (Chief Information Officer) Rodolfo O. Ploder also sold Equifax stock shares of an unknown value. Why? There are several reasons for speculation of such stock sale?

9. To provide relief for the Plaintiffs, who's PII has been compromised by the "Data Breach"; Plaintiff William H. Muscarella and Plaintiff Patricia R. Muscarella bring this action on behalf of themselves. They seek to recover actual and statutory damages, equitable relief, restitution and injunctive relief including an order requiring Equifax to improve [its] deplorable data security system/s and bring to an end [its] long history of "Data Breaches".

II. PARTIES

A. Plaintiffs

10. Plaintiff William H. Muscarella and Plaintiff Patricia R. Muscarella who both reside at 278 Spring Drive Roswell, Georgia. As a result, Equifax have possessed, managed, stored and controlled both Plaintiffs' financial history, including their "Social Security Numbers", birthdates, personal address, and other sensitive personal identify information (PII). Plaintiffs were victims of Equifax's "Data Breach" on or about Mid-May thru July of 2017.

11. Plaintiff William H. Muscarella and Plaintiff Patricia R. Muscarella who both reside at 278 Spring Drive Roswell, Georgia. As a result, Equifax have possessed, managed, stored and controlled both Plaintiffs' financial history, including their "Social Security Numbers", birthdates, personal address, and other sensitive personal identify information (PII). Plaintiffs were victims of Equifax's "Data Breach" on or about Mid-May thru July of 2017. (See Exhibit 1)

B. Defendants

12. Defendant Equifax Inc. is a multi-billion dollar company formed under the laws of the State of Georgia with its corporate headquarters in Atlanta, Georgia it provides credit information services to millions of businesses, governmental units, and [its] customers across the globe. Equifax operates through various subsidiaries/affiliates and agents, each of which entities acted as agents of Equifax, or in the alternative, in concert with Equifax.

13. Defendant Equifax Information Services LLC is a Georgia Limited Liability Company with [its] principal place of business located in Atlanta, GA. Equifax Information Services LLC conducted (and continues to conduct) business in the Northern District of Georgia.

III. Factual Allegations

to protect, shield, shelter, safeguard and preserve Plaintiff's PII from unauthorized access by third parties and to detect and stop any "Data Breach", to comply with laws implemented to preserve the "privacy rights" guaranteed under the FOURTH AMENDMENT of the CONSTITUTION of the UNITED STATES of AMERICA (dated on/or about September 17,1787) of this information, and to promptly notify Plaintiffs if/when their information was disclosed to an unauthorized third party.

15. Equifax knew or should have known that [its] failure to meet this duty, as well as [its] other numerous Fiduciary Duties and Federal and Georgia State laws/rules in regards to "Social Security Numbers" would cause substantial harm to Plaintiffs, including serious risks of credit harm and identity theft for years to come.

16. Equifax was well-aware, or reasonably should have been aware, the PII collected, amassed, controlled, stored, maintained and managed in Equifax's POS system/s and, Computer system/s and Data base/s were highly sensitive, susceptible to attack, and could be used for wrongful purposes by numerous third party and criminal elements, including identity theft and fraud. It is well known and the subject of many media reports that PII is highly sought and coveted and a frequent target of hackers. Prior to May 2017, Equifax had experienced at least three major cybersecurity incidents in which Plaintiff's PII information was compromised and accessed by unauthorized third parties.

17. Despite frequent public announcements of data breaches by U. S. government agencies, movie companies, corporate entities, foreign governments and including announcements made by Equifax itself, Equifax maintained an insufficient, inadequate, derisory, deficient, unsatisfactory and even laughable security system/s to protect, shield, safeguard and persevere the PII of Plaintiffs, in breach of [its] numerous Fiduciary duties to Plaintiffs. Given the Company's history of cyberattacks and [its] reputation as an industry leader in data breach security, Equifax could have and should have invested more money, time, and training of employees, equipment and resources into ensuring the security of [its] data base/s.

18. Because Equifax failed to maintain adequate safeguards, unauthorized third parties managed to exploit a weakness in Equifax's U. S. website application to gain access to sensitive data for roughly two months, beginning on or about mid-May 2017. The information accessed included Plaintiffs names; "Social Security Numbers", birth dates, addresses, and in some cases other PII personal information. In addition, credit card numbers of the Plaintiffs containing certain dispute documents with personal identifying information were also accessed.

19. The Equifax "Data Breach" was a direct and proximate result of Equifax's failure to properly safeguard/ shield and protect Plaintiff's and PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, and the common law, including Equifax's failure to establish and implement appropriate safeguards/shield to ensure the security and confidentiality of Plaintiff's' PII to protect and preserve against reasonable foreseeable threats to the security and integrity of such information, data and PII.

20. Equifax delayed informing Plaintiffs and the general public of the "Data Breach" and the question/s is "why" the delay? On or about July 29, 2017 and/or on or about September 7, 2017, Equifax announced to the public that it had discovered "unauthorized access" to [its] database/s, which jeopardized sensitive information for millions of people

21. As of this date, Equifax has yet to inform Plaintiffs directly whether their specific personal data was impacted and/or stolen by this massive security breach. Plaintiffs had to access a special Equifax web site, to verify, but received "no" written confirmation of such.

22. The direct consequences of Equifax's wrongful actions and/or inaction, [its] Board of Directors, [its] current and former employees and [its] failure to meet Equifax's Fiduciary Duty of Loyalty, Fiduciary Duty of Care, Fiduciary Duty of Obedience, Fiduciary Duty of Good Faith and Fair Dealing and Fiduciary Duty of Disclosure and duties to protect, shield, shelter, safeguard and preserve, and/or failing to maintain adequate security measures and/or failing to provide adequate resources, as well as prompt notice of the "Data

Breach". The Plaintiffs have been placed at an imminent, immediate, and continuing amplified risk and will continue to suffer substantial harm, including inconvenience, mental distress, debilitating worries, injury to their civil rights to "privacy" of their PII information, increased risk of fraud, further identity theft, and financial harm, the cost of monitoring their credit information to detect incidences of this and other possible losses consistent with the access of their PII by unauthorized third parties and/or criminal sources.

23. Armed with the stolen PII information of the Plaintiffs, unauthorized third parties and/or criminal elements now possess keys that unlock the Plaintiffs' medical histories, bank accounts, employee records and more. Abuse of sensitive credit and personal/private information can result in extensive and substantial harm to victims of security breaches. Criminals can take out loans, mortgage property, open financial accounts and credit card in a victim's name, obtain government benefit, file fraudulent tax returns, obtain medical services, and provide false information to police during an arrest, all under the victim's name.

24. Plaintiffs, who are senior citizens; now have to dedicate time, effort and money for protection, which Equifax should have provided as a respectable and trustworthy company in the first place. This effort will impose on their lives some of the following, inter alia, by placing "freezes" and alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time is lost forever and cannot be recaptured (especially when your age is 75 and 71). In all manners of life in this country (U.S.A.); time has constantly been recognized as compensable, for many people it is the way they are compensated, and even if retired from the work force, peoples should be free from having to deal with the consequences of a credit reporting agency's wrongful and reckless conduct, as is the case here.

25. Equifax's wrongful actions and/or in action directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' PII information, causing them to suffer, and continue to suffer, economic damages and other actual harm of which they are entitled to compensation, including:

a. violation of Plaintiffs' civil rights in regards to Fourth Amendment of U. S. Constitution;

b. theft of Plaintiffs' identities, which included all personal history and private financial information;

c. the imminent and certainly impending injury flowing from potential fraud;

d. future Identity theft posed by Plaintiffs' PII being place in general public and/or criminals hands;

e. sale of PII information being sold on the world black market;

f. loss of "privacy";

g. financial cost incurred by the "Data Breach" for repairs to or for the PII;

h. time and effort incurred to remedy or mitigate the effects of the "Data Breach";

i. ascertainable losses in the form of deprivation of the value of Plaintiffs' PII;

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of Plaintiffs' inability to use certain accounts and cards affected by the "Data Breach";

k. the loss of productivity and value of their time spent attempting to ameliorate, mitigate and deal with the actual and future consequences of the "Data Breach";

26. Because Equifax has demonstrated an inability to prevent a breach or stop it from continuing even after the breach was detected, Plaintiffs have an undeniable interest in insuring that their PII, which remains in Equifax's possession and control, is secure, remains secure, is properly and promptly destroyed as required and is not subject to further theft.

k. the loss of productivity and value of their time spent attempting to ameliorate, mitigate and deal with the actual and future consequences of the "Data Breach";

26. Because Equifax has demonstrated an inability to prevent a breach or stop it from continuing even after the breach was detected, Plaintiffs have an undeniable interest in insuring that their PII, which remains in Equifax's possession and control, is secure, remains secure, is properly and promptly destroyed as required and is not subject to further theft.

Count I

WILLFUL, VIOLATION of the FOURTH AMENDMENT of THE CONSTITUTION of the United States of America

27. Plaintiffs incorporate all preceding and subsequent paragraphs by reference.

28. Equifax knew or should have known that the Fourth Amendment of the Constitution of the United States of America (dated on or about September 17, 1787) provides that a Citizen of the United States of America has the right to "privacy". (See Exhibit 2)

Count II

WILLFUL, THEFT OF PLAINTIFFS' IDENITITY

29. Plaintiffs incorporate all preceding and subsequent paragraphs by reference.

30. Equifax Inc. "surreptitiously" collected and amassed, produced, controlled, stored and managed the Plaintiff's private, secret and personal information, material, data and history; as well as privileged financial records for at least 10 years or more "without" the verbal and/or written permission of the Plaintiffs. In other words, Equifax completed a total and complete theft of each of the "Plaintiff's Identities" via a system/s of reporting companies, banks and/or groups associated to/with Equifax for years. Equifax created, produced and managed a finely define system/s for tracking "everything" the Plaintiffs did in their personal and private and financial lives. Equifax controlled and managed and stored the "Identities" of the Plaintiffs on [its] computer system/s within Equifax control. Equifax then sold the Plaintiffs' personal and private and financial information and data, to whom ever would pay the "price" set for the enrichment of Equifax, [its] Board of Directors and [its] stockholders for various and numerous years. This system created by Equifax has made the Company in 2016, a 1.54 Billion dollar a year Company with tens of millions dollars of "profit" a year.

Count III

WILLFUL, VIOLATION OF THE GEORGIA AND/OR FEDERAL FAIR CREDIT REPORTING ACT

31. Plaintiffs incorporate all preceding and subsequent paragraphs by reference.

32. Plaintiffs are entitled to the protections of all Federal and Georgia State Fair Credit Reporting Acts.

33. Under Georgia State and/or Federal FCRA rules, a "consumer credit reporting agency" is defined as "any person who, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer reports to third parties.

34. Equifax is a consumer credit reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

35. As a consumer credit reporting agency, the Georgia State FCRA and/or Federal FCRA rules requires Equifax to "maintain reasonable procedures designed to...limit the furnishing of consumer credit reports to the purposes listed under section 1681b of this title."15 U. S. C. 1681 e (a).

36. Under Georgia State FCRA and/or Federal FCRA rules, a "credit report and/or file" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristic, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factoring establishing the consumer's eligibility for- (A) credit... to be used primarily for personal, family, or household purposes;...or (B) any other purpose authorized under section 1681b of this title.15 U. S. C. 1681a (d) (1). The compromised data was a consumer credit report under the Federal FCRA and/or Georgia State FCRA because it was a communication of information bearing on the Plaintiffs credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, of mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Plaintiffs eligibility for credit.

37. As a consumer credit reporting agency, Equifax may only furnish a credit report under the limited circumstances set forth in Federal 15 U.S.C.1681b, and 15 U.S.C. 1681b (a). None of the purposes listed under 15 U.S.C.1681b permit credit reporting agencies to furnish credit reports to unauthorized and/or unknown entities, or computer hackers such as those who accessed the Plaintiff's' PII. Equifax violated Federal 1681b by furnishing credit reports to unauthorized or unknown entities or computer hackers, as detailed above.

38. Equifax supplied Plaintiffs' credit reports by disclosing their credit reports to unauthorized entities and/or computer hackers; allowing unauthorized entities and computer hackers to access their credit reports; knowingly and/or recklessly failing to take security/s measures that would prevent unauthorized entities and/or computer hackers from accessing their reports; and/or failing to take reasonable security measures that would prevent unauthorized entities and/or computer hackers from accessing Equifax's/Plaintiff's credit reports. Another blatant example is on or about March 8, 2017 the U. S. Homeland Security Department "alerted" Equifax to an "online gap" in security of [its] computer system/s and/or data base/s. On or about October 3, 2017 Mr. Richard F. Smith (former Chief Executive Officer of Equifax) stated "but the Company did nothing" in testimony before House Energy Committee of the United States of America's. A further, example of complete failure is that Equifax's Board of Directors apparently never quizzed and/or questioned Mr. Richard F. Smith (former CEO) in regards to Susan Mauldin (a graduate of University of Georgia with a Bachelor's Degree and a Master of Fine Arts Degree in music composition) being hired as "Chief Security Officer" to safeguard/shield the Plaintiffs private personal information and secret financial data is beyond disbelief! It is perfectly clear; Equifax has demonstrated "contributory" act/s of negligence with a "willful and wanton" misconduct of negligence by "not" heeding U. S. Homeland Security Department's warning on or about March 8, 2017.

39. The Federal Trade Commission ("hereafter FTC") has pursued enforcement actions against consumer credit reporting agencies under the Federal FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in credit . "Let it be known", that the Plaintiffs have filed a complaint with the FTC in regards to Equifax's "Data Breach"; Complaint # 91065700 (see Exhibit 3) and filed a Incidents Report with the City of Roswell, Georgia Police Department Incident Report # 1712.001036 (see Exhibit 4). Additionally, City of Roswell Police department refused to permit the plaintiffs; to file a true, a complete and a comprehensive Incident report regarding Equifax's "Data Breach" which would have listed 13 State of Georgia statutory laws of which none are listed on Incident Report #1712.001036 and the Mayor of the City of Roswell has never responded to the Plaintiff's complaint letter (dated 1. 22.2018) (see Exhibit 5) regarding City of Roswell Police department actions.

40. Equifax willfully and recklessly violated Georgia State FCRA and Federal FCRA rules by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer credit reports to the purposes outlined under section1681b of the Federal FCRA guidelines. The contributory and willful and reckless nature of Equifax's violations is further supported by,

Act. 16C.F.R. Part 600, Appendix to Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties and responsibilities under the Georgia State and/or Federal FCRA. Any reasonable consumer credit reporting agency knows or should have known about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs of their rights under the Georgia State and Federal FCRA.

42. Equifax's willful and reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiff's PII for no permissible purposes under Georgia State and Federal FCRA rules.

43. Equifax's contributory action/s was for no permissible purposes under Georgia State and Federal FCRA.

COUNT IV

WILLFUL, VIOLATION OF THE GEORGIA BUSINESS PRACTICES ACT

44. Plaintiffs incorporate all preceding and subsequent paragraphs by reference.

45. While operating in Georgia, Equifax engaged in unfair and deceptive consumer acts in the conduct of trade and commerce in violation of O.C.G.A. 10-1-390 (a) and (b) by;

a. failing to adequately protects the PII of Plaintiffs from unauthorized disclosure, release, data breaches, and theft;

b. Failing to take proper action/s following known security risks and prior cybersecurity incidents;

c. Knowingly and fraudulently misrepresenting that Equifax would and could maintain adequate data security practices and procedures to safeguard/shield the Plaintiffs' PII from unauthorized disclosure, release, data breaches, and theft;

d. Knowingly omitting, suppressing, and concealing the inadequacy of Equifax's privacy and security protections for the Plaintiffs' PII;

e. Knowingly and fraudulently misrepresenting that Equifax would and could comply with the requirements of relevant Federal and Georgia State rules/laws pertaining to the privacy and security of the Plaintiffs' PII, including but not limited to duties imposed by the Federal FCRA, 15 U.S.C. 1681e, and the GLBA 15 U.S.C. 6801 et seq.

46. Further, the Georgia Fair Business Practices Act prohibits a person, firm or corporation from "making available to the general public" an individual's "Social Security Number", O.C.G.A. 10-1-393.8 (a) (1).

47. Equifax's failure to adequately protect/shield Plaintiffs' PII resulted in making the Plaintiffs' "social security numbers" available to third party computer hackers, and potentially the general public at the discretion of the third-party computer hackers now in possession of the PII.

48. Equifax's actions and its failures to act directly and proximately caused injury to the Plaintiffs, as discussed above.

49. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive and unscrupulous. These acts caused substantial injury to the Plaintiffs, which they could not reasonably avoid. This substantial injury outweighed any benefits.

50. Further, Equifax knew or should have known that [its] data security practices were derisory inadequate to safeguard/shield the Plaintiffs' PII. Equifax knew or should have known that the risk of a "Data Breach" or theft was highly likely. Equifax's actions, therefore, were contributory acts of negligence willful and wanton misconduct of negligence with respect to the rights of the Plaintiffs.

51. Defendants are subject to punitive damages under O.C.G.A. 51-12-5.1 (a) (b) (c) (d) because their conduct was contributory, willful, wanton, fraudulent, malicious, and/or oppressive; Further Equifax exhibited an entire want of care and loyalty which would raise the presumption of conscious indifference to consequences.

52. A written pre-suit demand under O.C.G.A. 10-1-399 (b) is unnecessary and unwarranted because Equifax has had notice, or it should have had notice of Plaintiffs' allegations, claims and demands, including from the filing of numerous underlying actions against it arising from the "Data Breach", the first of which were filed on or about September 8, 2017. Further, Equifax is the party with the most knowledge of the underlying facts giving rise to the Plaintiffs' allegations, so that any pre-suit notice would not put Equifax in a better position to evaluate those claims.

COUNT V

VIOLATION OF THE GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT

53. Plaintiffs incorporate all preceding and subsequent paragraphs by reference.

54. While, operating in Georgia, Equifax engaged in unfair and deceptive consumer acts in the conduct of trade and commerce in violation of O.C. G. A. 10-1-372 (a) (5) and (a) (7) by;

a. Knowingly and fraudulently misrepresenting that [its] credit reporting services had the benefit of data security practices and procedures adequate to protect Plaintiffs' PII from breach and theft. O.C.G.A. 10-1-372 (a) (5).

b. Knowingly and fraudulently misrepresenting that [its] credit reporting services were of a particular standard or quality, where Plaintiffs' PII would be adequately safeguarded. In fact Equifax's services met a much lower standard or quality, which directly and proximately resulted in breach of Plaintiff's PII. O.C.G.A. 10-1-372 (a) (7).

c. Knowingly and fraudulently omitting, suppressing, and concealing the inadequacy of [its] privacy and security protections for the Plaintiffs" PII O. C. G.A. 10-1-372 (a) (5), and (a) (7).

55. Equifax's actions and [its] failures to act directly and proximately caused injury to the Plaintiffs, as discussed above.

56. Defendants are subject to punitive damages under O. C.G.A. 51-12-5.1 because Equifax conduct was contributory, willful, wanton, fraudulent, malicious, and/or oppressive at the least; further Equifax exhibited an entire want of care and loyalty which would raise the presumption of conscious indifference to consequences.

COUNT VI

VIOLATION OF THE GEORGIA SECURITY BREACH NOTIFICATION ACT

57. Plaintiffs incorporate all preceding and subsequent paragraphs by reference;

58. Under O.C.G.A. 10-1-912 (b); "any information broker…that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery."

59. under O.C.G.A. 10-1-912 (b); "any person or business that maintains computerized data on behalf of an information broker… that includes personal information of individuals that the person or business does not

own shall notify the information broker... of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been acquired by an "unauthorized person."

60. Equifax is an information broker that owns or licenses computerized data that includes personal information, as defined by O.C.G.A. 10-1-911.

61. In the alternative, Equifax maintains computerized data (also known as a credit file and/or report) on behalf of an information broker that includes personal information that Equifax does not own, as defined by O.C.G.A. 10-1-911.

62. Plaintiffs' PII (including but not limited to names, addresses, Social Security numbers, possible Driver's license numbers includes personal information covered by O.C.G.A. 10-1-911 (6).

63. As stated above Equifax waited over a month to notify the public that any "Data Breach" had occurred. This failure to notify is a violation of Equifax's obligation to notify Plaintiffs of the breach under O.C.G.A. 10-1-912.

64. Equifax's failure to meet [its] statutory obligation directly and proximately caused injury to the Plaintiffs as discussed above.

65. Defendants are subject to punitive damages under O.C.G.A. 51-12-5.1 because their conduct was contributory, willful, wanton, fraudulent, malicious, and/or oppressive at the least; further Equifax exhibited an entire want of care/loyalty which would raise the presumption of conscious indifference to consequences.

COUNT VII

WILLFUL, CONTRIBUTORY NEGLIGENCE

66. Plaintiffs incorporate all preceding and subsequent paragraphs by reference;

67. Equifax owed a duty to Plaintiffs to exercise practical care in safeguarding their sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security system/s, protocols, and practices to ensure that Plaintiff's' PII information was adequately secured from unauthorized access.

68. Equifax owed a duty to Plaintiffs to implement intrusion detection processes that would detect a "Data Breach" in a timely manner.

69. Equifax also had a duty to delete any PII that was no longer needed to serve [its] client needs.

70. Equifax owed a duty to disclose, the material fact that [its] data security practices were inadequate to safeguard/shield Plaintiffs' PII.

71. Equifax had a special duty with Plaintiffs since Equifax had "surreptitiously" collected and amassed their PII. This provided or should have been an independent duty of care and loyalty. Moreover, Equifax had the ability to protect [its] system/s and the PII it produced, controlled, managed and stored (also known as a credit file and/or report) on [its] computer system/s and data base/s.

72. Equifax breached [its] Federacy duties as well as a duty of care and loyalty by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard/shield Plaintiffs' PII; (b) failing to detect and end the "Data Breach" in a timely manner; (c) failing to disclose that Defendants' data security practices were inadequate to safeguard/shield Plaintiffs' PII; and (d) failing to provide an adequate and timely notice of the breach.

73. Because of Equifax's breach of [its] duties, Plaintiff's PII has been accessed by unauthorized individuals.

74. Plaintiffs were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of [its] data security system/s would cause damages to Plaintiffs.

75. Equifax engaged in this contributory misconduct recklessly, in conscious neglect of Fiduciary duties and in callous indifference to consequences, and, in the alternative, with such want of care as would raise a presumption of a conscious indifference to consequences. Equifax was or should reasonably have been, aware of {its} contributory misconduct and of the foreseeable injury that would probably result, and with reckless indifference to consequences, consciously and intentionally committed the wrongful acts and commissions herein. Equifax's actions and omissions were, therefore, not just contributory negligent in nature, but reckless, willful, and wanton.

76. As a result of Equifax's contributory negligence, Plaintiffs suffered and will continue to suffer injury, inconvenience and exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs must now more closely monitor their financial accounts and credit histories to guard against further identity theft. Plaintiffs also have incurred, and will continue to incur on an indefinite basis, the threat of identity theft. The unauthorized acquisition of Plaintiffs' PII; has also diminished the value of the PII. Plaintiffs have also experienced other damages consistent with the theft of their PII and their personal Identities. Through Equifax's failure to timely discover and provide clear direct notification of the "Data Breach" to Plaintiffs, Equifax prohibited Plaintiffs from taking meaningful, proactive steps to secure their PII and personal identity.

77. The damages to Plaintiffs were a direct, proximate, reasonably foreseeable result of Equifax's breach of [its] Fiduciary duties.

78. Therefore, Plaintiffs are entitled to punitive damages in an amount to be proven at trial, that will summons and/or direct Equifax and [its] Board of Directors and others to obey Federal/States FCRA laws/rules and to fulfill their Fiduciary Duty of Loyalty, Fiduciary Duty of Care, Fiduciary Duty of Obedience, Fiduciary Duty of Good Faith and Fair Dealing and Fiduciary Duty of Disclosure and to protect, shield, shelter, safeguard and preserve Plaintiffs' PII from personal and financial harm as well as "Identity Theft".

COUNT VIII

CONTRIBUTORY NEGLIGENCE PER SE

79. Plaintiffs incorporate all proceeding and subsequent paragraphs by reference;

80. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect PII data/information.

81. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained, managed and stored, and the foreseeable consequences of a "Data Breach" at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiffs.

82. Equifax's violation of Section 5 of the FTC Act constitutes negligence per se.

83. Equifax also violated the FCRA, as stated in Counts I and II. Equifax's violation of the FCRA constitutes negligence per se.

84. The Federal Gramm-Leach-Bliley Act ("hereafter GLBA") requires covered entities to satisfy certain standards relating to administrative, technical, and physical safeguards: (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such

records or information which could result in substantial harm or inconvenience to any customer. 15 U.S.C. § 6801(b). Case 1:17-cv-03659-MHC Document 1 Filed 09/20/17 Page 27 of 36.

85. Businesses subject to the GLBA "should take preventative measures to safeguard customer information against attempts to gain unauthorized access to the information." Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F.

86. In order to satisfy their obligations under the GLBA, Equifax was required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer's information at issue." See 16 C.F.R. § 314.3; see also Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F. (Subject companies must "design [its] information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the...company's activities"). This obligation included considering and, where the Company determined appropriate, adopting mechanisms for "encryption of electronic customer's (Plaintiffs') information, including while in transit or in storage on networks and/or system/s to which unauthorized individuals may have access."

87. In addition, under the interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to [its] data base information and information systems." "The program should be appropriate to the size and complexity of the institution and the nature and scope of [its] activities.

88. Equifax had a fiduciary duty and affirmative duty to protect their computer system/s against unauthorized access or use. Timely notification to Plaintiffs in the event of a "Data Breaches" Case 1:17-cv-03659-MHC Document 1 Filed 09/20/17 Page 28 of 36 is important to meeting this fiduciary duties and affirmative obligation. Accordingly, when Equifax became aware of "unauthorized access to sensitive data base information," it should have conducted a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notified the affected people as soon as possible." Sensitive customer information includes much of the Plaintiffs PII released in the "Data Breach".

89. Equifax violated the GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any sensitive information at issue." This includes, but is not limited to, (a) Equifax's failure to implement and maintain adequate data security practices to safeguard Plaintiffs' PII; (b) failing to detect the "Data Breach" in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Plaintiff's PII.

90. Equifax also violated the GLBA by failing to notify affected Plaintiffs as soon as possible after it became aware of unauthorized access to sensitive customer information.

91. Equifax's violations of the GLBA constitute contributory negligence per se.

92. Equifax also violated Georgia Security Breach Notification Act ("hereafter GSBNA"), O.C.G.A. § 10-1912, et seq. The act provides that "any information broker ... that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery." Further, this "notice shall be made in the most expedient time possible and without unreasonable delay ... " Under O.C.G.A. § 10-1- 912 (b), "any person or business that maintains computerized data on behalf of an information broker ... that includes personal information of individuals that the person or business does not Case 1:17-cv-03659-MHC Document 1 Filed 09/20/17 Page 29 of 36 own shall notify the information broker ... of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been acquired by an unauthorized person."

93. Defendants violated the GSBNA by failing to conduct an adequate investigation to identify the breach, failing to promptly determine whether there had been a breach, and failing to notify Plaintiffs of the breach in the most expedient manner possible. Defendants failed to discover the breach for over two months. They then waited over a month to release a statement that any breach had occurred.

94. Plaintiffs are that which the FTC Act, the FCRA, the GLBA, and the GSBNA were intended to protect.

95. Plaintiffs were foreseeable victims of Equifax's violation of the FTC Act, the FCRA, the GLBA, and the GSBNA. Equifax knew or should have known that [its] failure to take reasonable measures to prevent a breach of [its] data security system/s, and failure to timely and adequately report it directly to the Plaintiffs.

96. The harm that occurred as a result of the Equifax "Data Breach" is the type of harm the FTC Act, the FCRA, the GLBA, and the GSBNA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs.

97. Equifax engaged in this contributory misconduct recklessly, in conscious contributory neglect of duties and in callous indifference to consequences, and, in the alternative, with such want of care as would raise a presumption of a conscious indifference to consequences. Equifax was or should know about Case 1:17-cv-03659-MHC Document 1 filed 09/20/17 Page 30 of 36 and aware of [its] willful, mindful and wanton contributory misconduct. Mindful of the foreseeable injury that would probably result, and with reckless indifference to consequences, consciously and intentionally committed the wrongful acts and omissions herein. Equifax's actions and omissions were, therefore, demonstrated contributory negligence and were grossly reckless, willful, and wanton with Plaintiffs PII.

98. As a direct and proximate result of Equifax's contributory negligence per se, Plaintiffs have suffered and will continue to suffer injury. Equifax's did not include adequate and/or industry standard data protection, inconvenience and exposure to a heightened, imminent risk of fraud, identity theft, and financial harm to Plaintiffs. Plaintiffs now must more closely monitor their financial accounts and credit histories to guard against identity theft. Plaintiffs have incurred, and will continue to incur on an indefinite basis, an investment of time for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition (theft) of Plaintiffs' PII has also diminished the value of the PII. Plaintiffs have also experienced other damages consistent with the theft of their PII. Through [its] failure to timely discover and provide clear and/or direct personal notification of the "Data Breach" to Plaintiffs, Equifax prohibited Plaintiffs from taking meaningful, proactive steps to secure their PII.

99. But for Equifax's violation of the applicable statutory laws and regulations, Plaintiffs PII would not have been accessed (stolen) by unauthorized individuals.

100. The damages to Plaintiffs were a direct, proximate, reasonably foreseeable result of Equifax's breaches of the applicable laws and regulations. Case 1:17-cv-03659-MHC Document 1 Filed 09/20/17 Page 31 of 36 136. Therefore, Plaintiffs are entitled to damages in an amount to be proven at trial.

COUNT VIIII UNJUST ENRICHMENT

101. Plaintiffs incorporate all preceding and subsequent paragraphs by reference.

102. Equifax received payment to perform services that included protecting Plaintiffs' PII. Equifax failed to do this, but retained Equifax's direct customer's (banks-etc.) payments.

103. Equifax retained the benefit of said payments under circumstances which renders it inequitable and unjust for Equifax to retain such benefits without paying for their value, since all of the PII data stored in [its] computer system/s is not "owned" by Equifax; it is the property of the Plaintiffs.

104. Defendants have knowledge of said benefits.

105. Plaintiffs are entitled to recover damages in an amount to be proven at trial.

COUNT X DECLARATORY JUDGMENT

106. Plaintiffs incorporate all preceding and subsequent paragraphs by reference.

107. Equifax owes duties of care to Plaintiffs that require it to adequately secure PII.

108. Equifax still possesses PII pertaining to Plaintiffs.

109. Equifax has made no announcement or notification that it has remedied the vulnerabilities in [its] computer data system/s, and, most importantly, [its] security system/s.

110. Accordingly, Equifax has not satisfied [its] contractual obligations and statutory legal duties to Plaintiffs and/or Fiduciary duties. In fact, now that Equifax's slipshod approach towards data security Case 1:17-cv-03659-MHC Document 1 Filed 09/20/17 Page 32 of 36 has become public, the PII in [its] possession is more vulnerable than previously.

111. Equifax's breach of [its] contractual obligations and duties of care, will caused Plaintiffs personal and financial harm for an unknown number of years.

112. Plaintiffs, therefore, seek a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations, duties of care and fiduciary duties and (b) in order to comply with [its] contractual obligations and duties of care, Equifax must implement and maintain realistic security measures, including, but not limited to: a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third party security auditors; (c) engaging third-party security auditors and internal personnel to run automated security monitoring;(d). auditing, testing, and training its security personnel regarding any new or modified procedures; (e) segmenting PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems; (f) purging, deleting, and destroying many reasonable secure manner PII not necessary for its provisions of services; f. conducting regular database scanning and securing checks; Case 1:17-cv-03659-MHC Document 1 Filed 09/20/17 Page 33 of 36 (g) routinely and continually conducting internal training and education/training to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (h.) educating [its] customers about the threats they face as a result of the loss of their financial and personal information to third parties.

113. In addition, Georgia has adopted the Model Business Corporation Act (hereafter MBCA). It is sufficient to say that the Fiduciary duty of Officers and Directors at "Equifax" is generally subdivide into the Duty of Care and the Duty of Loyalty. The MBCA section 8.30 defines a corporate director's a Duty of Care and MBCA section 8.42 imposes substantially the same Duty of Care on corporate Officers possessing "discretionary" authority. These two sections focus on the manner in which Directors and Officers perform their duties, "not" the correctness of their decisions. Directors and Officers are required to perform their duties in good faith, with the care of ordinarily prudent persons in like positions and in a manner that they believe to be in the best interest of the corporation. It is clear that Equifax's Board of Directors and [its] Officers did "fail" in their Fiduciary Duties of Care and Fiduciary Duties of Loyalty in regards to the Plaintiffs by "not" protecting them from a "Data Breach". It is also "clear" that Equifax's Board of Directors and [its] officers did "fail" by "not" protecting the Plaintiffs from a "Data Breach" by employing Susan Mauldin as "Chief Security Officer" with "no" apparent experience and/or training in regards to Data Security and/or Data Security Systems.

PRAYER FOR RELIEF ON INDIVIDUAL WHEREFORE, the Plaintiffs on their own behalf pray that this Court: (1) Declare and adjudge that Defendants' policies, practices, actions and procedures challenged herein are illegal and in violation of the civil rights of the Plaintiffs; (2) Issue a permanent injunction against Defendants and their partners, Board of Directors, officers, trustees, owners, employees, agents, attorneys, successors, assigns, representatives, and any and all persons acting in concert with them from engaging in any conduct violating the rights of Plaintiffs, and those similarly situated to them; (3) Order injunctive relief requiring Defendants to (a) strengthen their data security system/s that maintain PII to comply with the applicable Federal/State laws alleged herein and "best practices" under industry standards; (b) engage third-party auditors and internal personnel to conduct security testing and audits on Defendants' systems on a periodic Case 1:17-cv-03659-MHC Document 1 Filed 09/20/17 Page 34 of 36 basis; (c) promptly correct any problems or issues detected by such audits and testing; and (d) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a "Data Breach", and how to appropriately respond; (4) Award compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement to Plaintiffs in an amount to be determined at trial; (5) Award punitive damages under O.C.G.A. § 51-12-5.1 and other applicable law; (6) Order Defendants to make the Plaintiffs whole by providing them with any other monetary and affirmative relief; (7) Award Plaintiffs their litigation costs and expenses, including, but not limited to, reasonable attorneys' fees; (8) Award Plaintiffs all pre-judgment interest and post-judgment interest available under law; (9) Award Plaintiffs any other appropriate equitable relief; (10) Order that this Court retain jurisdiction of this action until such time as the Court is satisfied that the Defendants have remedied the practices complained of herein and are determined to be in full compliance with the law; and Case 1:17-cv-03659-MHC Document 1 Filed 09/20/17 Page 35 of 36 (11) Award additional and further relief as this Court may deem just and proper.

The Plaintiffs request an expedite trial date, due to their age (75 and 71 years) and health.

JURY DEMAND

Plaintiffs demand a trial by jury on all issues triable of right by jury.

(https://www.equifax.com)

Thank You

Based on the information you provided, our records indicate your personal information was impacted by this incident.

Click the button below to continue your enrollment in TrustedID Premier.

Enroll

For more information visit the FAQ page. (https://faq.trustedidpremier.com)

Exhibit [redacted] 2

The Fourth Amendment originally enforced the notion that "each man's home is his castle", secure from unreasonable searches and seizures of property by the government. It protects against arbitrary arrests, and is the basis of the law regarding search warrants, stop-and-frisk, safety inspections, wiretaps, and other forms of surveillance, as well as being central to many other criminal law topics and to privacy law.

Subject: Complaint has been submitted

From: no-reply@consumersentinel.gov (no-reply@consumersentinel.gov)

To: Redacted

Date: Friday, December 15, 2017 4:41 AM

Complaint Submitted - Your reference number is: Redacted

Thank you for contacting the Federal Trade Commission. We have given your complaint the reference number listed above. Please use that reference number if you need to contact us about your complaint in the future.

Once we have reviewed your complaint, you may receive another email with additional information that may further assist you.

Here are link(s) to the publications you may find useful: **10 Ways to Avoid Fraud**

INCIDENT/INVESTIGATION REPORT

Agency Name: *Roswell Police Department*
ORI: *GA0600500*
Case#: Redacted
Date / Time Reported: *12/26/2017 12:27 Tue*
Last Known Secure: *05/13/2017 08:00 Sat*
At Found: *12/26/2017 12:27 Tue*

INCIDENT DATA

Location of Incident: *278 Spring Dr, Roswell GA 30075-*
Premise Type: *Residence / Home*
Zone/Tract: B2

#1	Crime Incident(s): *Miscellaneous Information-no Offense 0009* (Att)	Weapon / Tools: *NOT APPLICABLE/NONE*			Activity
		Entry	Exit	Security	
#2	Crime Incident ( )	Weapon / Tools			Activity
		Entry	Exit	Security	
#3	Crime Incident ( )	Weapon / Tools			Activity
		Entry	Exit	Security	

MO:

VICTIM

of Victims: *0* Type: Injury: Domestic: N

	Victim/Business Name (Last, First, Middle)	Victim of Crime #	DOB / Age	Race	Sex	Relationship To Offender	Resident Status	Military Branch/Status
V1								

Home Address: Home Phone:
Employer Name/Address: Business Phone: Mobile Phone:

VYR	Make	Model	Style	Color	Lic/Lis	VIN

OTHERS INVOLVED

CODES: V- Victim (Denote V2, V3) O = Owner (if other than victim) R = Reporting Person (if other than victim)

Type: INDIVIDUAL(NON LE) Injury:

Code	Name (Last, First, Middle)	Victim of Crime #	DOB / Age	Race	Sex	Relationship To Offender	Resident Status	Military Branch/Status
RP	*MUSCARELLA, WILLIAM HOWARD*		[redacted]1942 Age 75	W			*Resident*	

Home Address: *278 Spring Dr Roswell, GA 30075* Home Phone: Redacted
Employer Name/Address: *N/A (N/A)* Business Phone: Mobile Phone: [redacted]

Type: INDIVIDUAL(NON LE) Injury:

Code	Name (Last, First, Middle)	Victim of Crime #	DOB / Age	Race	Sex	Relationship To Offender	Resident Status	Military Branch/Status
IO	*MUSCARELLA, PATRICIA RUTH*		[redacted]1946 Age 71	W	F		*Resident*	

Home Address: *278 Spring Dr Roswell, GA 30075* Home Phone: Redacted
Employer Name/Address: *RETIRED* Business Phone: Mobile Phone: [redacted]

PROPERTY

1 = None 2 = Burned 3 = Counterfeit / Forged 4 = Damaged / Vandalized 5 = Recovered 6 = Seized 7 = Stolen 8 = Unknown ("OJ" = Recovered for Other Jurisdiction)

VI #	Code	Status Frm/To	Value	OJ	QTY	Property Description	Make/Model	Serial Number

Officer/ID#: *DE CRESCENTE, A. M. (637)*
Invest ID#: *(0)*
Supervisor: *CARR, K. (129)*
Complainant Signature:
Case Status: *Active* *12/26/2017*
Case Disposition:

R_CS1IBR Printed By: LAPT, Sys#: 1303028 01/03/2018 12:19

INCIDENT/INVESTIGATION REPORT

Roswell Police Department

Case # Redacted

Status Codes 1 = None 2 = Burned 3 = Counterfeit / Forged 4 = Damaged / Vandalized 5 = Recovered 6 = Seized 7 = Stolen 8 = Unknown

	IBR	Status	Quantity	Type Measure	Suspected Type	
DRUGS						

Assisting Officers

Suspect Hate / Bias Motivated:

INCIDENT/INVESTIGATION REPORT

Narr. (cont.) OCA: 1712-001036 *Roswell Police Department*

NARRATIVE

On December 26, 2017, at approximately 12:47 hours, I, Officer De Crescente, responded to 39 Hill Street in reference to a possible financial identity fraud call. I met with the reporting parties, WILLIAM MUSCARELLA and PATRICIA MUSCARELLA (residents at 278 Spring Dr.), who informed me that Equifax notified them that each of their identities had been compromised in the Equifax information breech on May 13, 2017. Neither party has noticed any fraudulent activity on their credit up until this point. I advised both parties to put a freeze on their credit in order to reduce the risk of future fraudulent activity. No crime was committed, reporting parties merely wanted to document the occurrence.

INCIDENT/INVESTIGATION REPORT

Agency Name	Roswell Police Department
ORI	GA0600500
Case#	Redacted
Date / Time Reported	12/26/2017 12:27 Tue
Last Known Secure	05/13/2017 08:00 Sat
At Found	12/26/2017 12:27 Tue
Location of Incident	278 Spring Dr, Roswell GA 30075-
Premise Type	Residence / Home
Zone/Tract	B2

#1	Crime Incident(s) (Att) Miscellaneous Information-no Offense 0009	Weapon / Tools NOT APPLICABLE/NONE			Activity
		Entry	Exit	Security	
#2	Crime Incident ( )	Weapon / Tools			Activity
		Entry	Exit	Security	
#3	Crime Incident ( )	Weapon / Tools			Activity
		Entry	Exit	Security	

# of Victims 0 | Type: | Injury: | Domestic: N

V1	Victim/Business Name (Last, First, Middle)	Victim of Crime #	DOB / Age	Race	Sex	Relationship To Offender	Resident Status	Military Branch/Status

Home Address | Home Phone

Employer Name/Address | Business Phone | Mobile Phone

VYR	Make	Model	Style	Color	Lic/Lis	VIN

CODES: V- Victim (Denote V2, V3) O = Owner (if other than victim) R = Reporting Person (if other than victim)

Type: INDIVIDUAL(NON LE) | Injury:

Code	Name (Last, First, Middle)	Victim of Crime #	DOB / Age	Race	Sex	Relationship To Offender	Resident Status	Military Branch/Status
RP	MUSCARELLA, WILLIAM HOWARD		[redacted]1942 Age 74	W			Resident	

Home Address: 278 Spring Dr Roswell, GA 30075 | Home Phone: Redacted

Employer Name/Address: N/A (N/A) | Business Phone | Mobile Phone: [redacted]

Type: INDIVIDUAL(NON LE) | Injury:

Code	Name (Last, First, Middle)	Victim of Crime #	DOB / Age	Race	Sex	Relationship To Offender	Resident Status	Military Branch/Status
IO	MUSCARELLA, PATRICIA RUTH		[redacted]1946 Age 71	W	F		Resident	

Home Address: 278 Spring Dr Roswell, GA 30075 | Home Phone: Redacted

Employer Name/Address: RETIRED | Business Phone | Mobile Phone: [redacted]

1 = None 2 = Burned 3 = Counterfeit / Forged 4 = Damaged / Vandalized 5 = Recovered 6 = Seized 7 = Stolen 8 = Unknown ("OJ" = Recovered for Other Jurisdiction)

VI #	Code	Status Frm/To	Value	OJ	QTY	Property Description	Make/Model	Serial Number

Officer/ID# DE CRESCENTE, A. M. (637)

Invest ID# (0) | Supervisor CARR, K. (129)

Complainant Signature | Case Status Active 12/26/2017 | Case Disposition:

R_CS11BR Printed By: LAPT, Sys#: 1303028 01/09/2018 14:17

INCIDENT/INVESTIGATION REPORT

Roswell Police Department

Case # Redacted

Status Codes 1 = None 2 = Burned 3 = Counterfeit / Forged 4 = Damaged / Vandalized 5 = Recovered 6 = Seized 7 = Stolen 8 = Unknown

	IBR	Status	Quantity	Type Measure	Suspected Type	
DRUGS						

Assisting Officers

Suspect Hate / Bias Motivated:

INCIDENT/INVESTIGATION REPORT

Narr. (cont.) OCA: 1712-001036 *Roswell Police Department*

NARRATIVE

On December 26, 2017, at approximately 12:47 hours, I, Officer De Crescente, responded to 39 Hill Street in reference to a possible financial identity fraud call. I met with the reporting parties, WILLIAM MUSCARELLA and PATRICIA MUSCARELLA (residents at 278 Spring Dr.), who informed me that Equifax notified them that each of their identities had been compromised in the Equifax information breech on May 13, 2017. Neither party has noticed any fraudulent activity on their credit up until this point. I advised both parties to put a freeze on their credit in order to reduce the risk of future fraudulent activity. No crime was committed, reporting parties merely wanted to document the occurrence.

Date: 1.22.2018

To: Mayor City of Roswell, Georgia

From: William H. Muscarella

Patricia R. Muscarella

Subject: Police Incident/Investigation Report

Number: Redacted

Attn: Mayor Lori Henry

Dear Mayor,

I had a very distressing experience with the City of Roswell's-Georgia, U. S. A.; Police department in regards to filling out an incident/investigation report regarding the theft of our Identity by Equifax Inc. I have been to the Roswell Police department three times, since 12.26.17. On the first trip, we tried to file an Identity Theft report with Officer De Crescente; we explained that Equifax Inc. had stolen our Identity. I provided data in writing proving, that was in fact the case. Officer De Crescente looked at the paper work and handed it back to me. Officer De Crescente did not seem to be interested in our problem and just wanted us to leave. Officer De Crescente wrote up a report and said to pick it up in 3 to 5 days.

I returned to the Roswell police station and received the report, which stated on the report Block #1 the following, "Crime Incident(s) Miscellaneous Information-no Offense 0009". (See attachment 1)

I when over to main office of the Roswell police station, and made a formal complaint, regarding the report was neither true nor accurate. It took some time, when a Sargent appeared. I explained the problem, after some more time Officer De Crescente arrived in the lobby of the City of Roswell Police station.

I again explained that report, was not what my wife and I had reported on 12.26.2017. We had a very "difficult" conversation; Officer De Crescente was very "aggravated", that I wanted the report to show that Equifax Inc. did in deed steal our Identities. I gave a list of three Georgia laws that Equifax Inc. had violated. Officer De Crescente stated "I will look these up" in a foul manner. I stated, "Yes, please do and I expect that you will". Officer De Crescente stated "the report will be ready in 3 to 5 days (see attachment 3).

I again returned to Roswell Police station on 1.9.2018, to retrieve the new report. I found that the "new" Incident/Investigation report was basically the same as the first one, with a few new words. No Georgia laws were listed on the report that Equifax Inc. had violated. The report made "no" reference to any Georgia laws that I had given to Officer De Crescente. I have attached copy of the report identified by # Redacted (See attachment 2).

I now will list for your review all of the Georgia Laws that Equifax Inc. has violated in 2017, below.

O. C. G. A. 10-1-390 (a) and (b)

O. C. G. A. 10-1-393.8 (a) (1)

O. C. G. A. 51-12-5.1 (a) (b) (c) (d)

O. C. G. A. 10-1-372 (a) (5) and (a) (7)

O. C. G. A. 10-1-372 (a) (5)

O. C. G. A. 10-1-372 (a) (7)

O. C. G. A. 51-12-5.1

O. C. G. A. 10-1-912 (b)

O. C. G. A. 10-1-911 (6)

O. C. G. A. 10-1-912

O. C. G. A. 10-1912

O. C. G. A. 10-1912 (b)

In addition, please note that Officer De Crescente requested, that I not to give any Federal laws, which I did not, but there are many. Officer De Crescente stated "That Equifax Inc. was not in Roswell area of authority. I replied "Yes, I understand and that is OK, I just want the Georgia laws listed on the report".

If Officer De Crescente had looked up the laws as she stated, then she would have found the same 12 laws listed above or at least the 3 laws, I gave her and one more below.

In addition, Georgia Department of Law (Consumer Protection Unit) stated (on [its] web site) "File a police report with your local police agency. In Georgia, "Identity Theft" is a felony under Official Code of Georgia Annotated Section 16-9-121". See attachment

I am requesting that you as Mayor of the City of Roswell please assist me in this endeavor.

Please advise what I must do as a loyal citizen of the United States of America and of the City of Roswell, Georgia for many years, a Senior citizen and a Veteran. I feel as the City of Roswell Police department has not performed according to their oath of office and loyalty owed to citizens of Roswell, Georgia.

I would also, like to mention this is not the "first" problem, with the City of Roswell Police department. A few years ago, one of the officers stated he would arrest my wife for making a false Police report that the IRS had instructed us to do.

I have spoken to the Attorney General Office of Georgia, District Attorney Office of Fulton County, Georgia Bureau of Investigation and I hope that I do not have to go public with this embarrassing problem for the citizens of Roswell, Georgia.

I would also like a copy of the City of Roswell Official "Oath of Office" all police officers swear to, when becoming a police officer for the City of Roswell and [its] citizens.

I will leave this in your hands for a few days.

Best regards,

William H. Muscarella

Patricia R. Muscarella

Redacted

Redacted

Hand Delivered Letter 1.22.2018 in Mayor's Office City of Roswell, GA.

Received by _____ Date_____ Time_____